IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

ANDREW LEONARD, NICHOLAS DEGRASSE, JAMES FRAZIER, AND CHARLES FRYE, individually and on behalf of all others similarly situated, Plaintiffs, v. MCMENAMINS, INC., Defendant.	Cause No.: 2:22-cv-00094-BJR PLAINTIFFS' FIRST AMENDED CLASS ACTION COMPLAINT **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Cindy Heidelberg, WSBA #44121
BRESKIN JOHNSON & TOWNSEND, PLLC
1000 Second Avenue, Suite 3670
Seattle, WA 98104
(206) 652-8660 Fax (206) 652-8290
cheidelberg@bjtlegal.com

Nicholas A. Migliaccio (*pro hac vice*)
Jason S. Rathod (*pro hac vice*)
MIGLIACCIO & RATHOD LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Plaintiffs Andrew Leonard, Nicholas deGrasse, James Frazier, and Charles Frye ("Plaintiffs"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby allege the following against Defendant McMenamins, Inc. ("McMenamins" or "Defendant").

NATURE OF THE ACTION

1. This is a class action for damages with respect to McMenamins, Inc., for its failure to exercise reasonable care in securing and safeguarding their employees' sensitive information—including names, addresses, email addresses, telephone numbers, dates of birth, disability status, Social Security numbers, health insurance information, medical notes, and direct deposit bank account information collectively known as personally identifiable information collectively known as personally identifiable information ("PII" or "Private Information").

2. This class action is brought on behalf of individuals employed by McMenamins between January 1, 1998 and December 12, 2021 who had their sensitive PII accessed by unauthorized parties due to inadequate network security in a ransomware attack on McMenamins' IT systems on or around December 12, 2021 (the "Data Breach").

3. The Data Breach affected the data of past and present McMenamins employees in at least two states.

4. McMenamins reported to Plaintiffs that information compromised in the Data Breach included their PII.

5. As a result of the Data Breach, Plaintiffs and other Class members will continue to experience various types of misuse of their PII in the coming years, including but not limited to unauthorized credit card charges, unauthorized access to email accounts, unauthorized use of bank account information, including routing and account numbers, and other fraudulent use of their financial and professional information.

6. There has been no assurance offered from McMenamins that all personal data or copies of data have been recovered or destroyed. McMenamins offered 12 months of Experian

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

IdentityWorks credit monitoring, which does not guarantee the security of Plaintiffs' information. To mitigate further harm, Plaintiffs chose not to disclose any more information to receive these services connected with McMenamins.

7. Accordingly, Plaintiffs assert claims for negligence, breach of contract, breach of implied contract, breach of fiduciary duty, violations of the Washington Consumer Protection Act—Wash. Rev. Code An. §§ 19.86.020, *et seq.*, and declaratory relief.

PARTIES

A. Plaintiff Andrew Leonard

8. Plaintiff Andrew Leonard is a resident of Bothell, Washington, and brings this action in his individual capacity and on behalf of all others similarly situated. Plaintiff Leonard was an employee of McMenamins' Bagdad Theater & Pub in Portland, Oregon, as well as the McMenamins' Anderson School facility in Bothell, Washington from 2015 to 2019. As a condition of employment at McMenamins Anderson School, Plaintiff Leonard was required to provide McMenamins with his PII, including direct deposit banking information, which McMenamins then maintained in its human resources/ payroll files. In maintaining his information, Defendant expressly and impliedly promised to safeguard Plaintiff Leonard's PII. Defendant, however, did not take proper care of Mr. Leonard's PII, leading to its exposure as a direct result of Defendant's inadequate security measures. In January of 2022, Plaintiff Leonard received a notification letter dated December 30, 2021 from Defendant stating that his PII was stolen, which included Mr. Leonard's "name, address, telephone number, email address, date of birth, race, ethnicity, gender, disability status, medical notes, performance and disciplinary notes, Social Security number, health insurance plan election, income amount, and retirement contribution amounts." The letter also noted the possibility of the hackers accessing or removing records that included direct deposit bank account information.

9. The letter also offered one year (12 months) of credit monitoring through Experian IdentityWorks, which was and continues to be ineffective for Leonard and other Class members.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

The Experian credit monitoring would have shared Mr. Leonard's information with third parties and could not guarantee complete privacy of his sensitive PII.

10. In the months and years following the Data Breach, Mr. Leonard and the other Class members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, requests for services taken out in employees' names, fraudulent bank account charges, and targeted advertising without consent.

11. Plaintiff Leonard greatly values his privacy, especially in the administration of his finances, and would not have given his PII to McMenamins if he had known that it was going to maintained in McMenamins' database without adequate protection.

B. Plaintiff Nicholas deGrasse

12. Plaintiff Nicholas deGrasse is a resident of Kirkland, Washington, and brings this action in his individual capacity and on behalf of all others similarly situated. Plaintiff deGrasse was a food runner at the McMenamins' Anderson School facility in Bothell, Washington from 2016 to 2019. As a condition of employment at McMenamins, Plaintiff deGrasse was required to provide McMenamins with his PII, including his Social Security number and other financial information such as his direct deposit bank account information, which McMenamins then maintained in its human resources/payroll files. In maintaining his information, Defendant expressly and impliedly promised to safeguard Plaintiff deGrasse's PII. Defendant, however, did not take proper care of Mr. deGrasse's PII, leading to its exposure as a direct result of Defendant's inadequate security measures.

13. In the months and years following the Data Breach, Mr. deGrasse and the other Class members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, requests for services taken out in employees' names, fraudulent bank account charges, and targeted advertising without consent.

14. Some of these harms have already materialized in Mr. deGrasse's case. In January of 2022, unauthorized individuals charged Mr. deGrasse's Visa credit card account for more than

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

$1000 under multiple merchant names around in several countries through a mix of retailers and services, including a charge under the merchant ID "genius flights LLC" that Mr. deGrasse neither authorized nor approved in any way. Although none of these charges were billed to him in a credit card statement, these fraudulent attempts to charge his card led Mr. deGrasse to spend approximately 1.5 hours canceling these fraudulent charges with Visa customer representatives and activating a new credit card. The contact information Plaintiff deGrasse registered this credit card with was the same contact information he used to register his information with McMenamins as an employee, including his name, address, phone number, and Social Security number.

15. Plaintiff deGrasse greatly values his privacy, especially in the administration of his finances, and would not have agreed to give his information to McMenamins if he had known that it was going to be maintained using inadequate data security measures.

C. Plaintiff James Frazier

16. Plaintiff James Frazier is a resident of Vancouver, Washington, and brings this action in his individual capacity and on behalf of all others similarly situated. Plaintiff Frazier was a host, food runner, and bar manager at McMenamins' Edgefield Hotel location in Troutdale, Oregon, from 2019 to 2021. As a condition of employment at McMenamins, Plaintiff Frazier was required to provide McMenamins with his PII, including his Social Security number and other financial information such as his direct-deposit bank account information, which McMenamins then maintained in its human resources/payroll files. In maintaining his information, Defendant expressly and impliedly promised to safeguard Plaintiff Frye's PII. Defendant, however, did not take proper care of Mr. Frazier's PII, leading to its exposure as a direct result of Defendant's inadequate security measures. In December of 2021, Plaintiff Frazier received a notification letter from Defendant stating that his PII was stolen, which included Mr. Frazier's "name, address, telephone number, email address, date of birth, race, ethnicity, gender, disability status, medical notes, performance and disciplinary notes, Social Security number, health insurance plan election,

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

income amount, and retirement contribution amounts." The letter also noted the possibility of the hackers accessing or removing records that contained direct deposit bank account information.

17. The letter also offered one year (12 months) of credit monitoring through Experian IdentityWorks, which was and continues to be ineffective for Mr. Frazier and other Class members.

18. In the months and years following the Data Breach, Mr. Frazier and the other Class members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, requests for services taken out in employees' names, fraudulent bank account charges, and targeted advertising without consent.

19. Plaintiff Frazier greatly values his privacy, especially in the administration of his finances, and would not have given his PII to McMenamins if he had known that it was going to maintained in McMenamins' database without adequate protection.

D. Plaintiff Charles C. Frye

20. Plaintiff Frye is a resident of Portland, Oregon, and brings this action in his individual capacity and on behalf of all others similarly situated. Plaintiff Frye is a current employee of McMenamins' Bagdad Theater & Pub in Portland, Oregon. As a condition of employment at McMenamins, Plaintiff Frye was required to provide McMenamins with his PII, including his Social Security number and other financial information such as his direct-deposit bank account information, which McMenamins then maintained in its human resources/ payroll files. In maintaining his information, Defendant expressly and impliedly promised to safeguard Plaintiff Frye's PII. Defendant, however, did not take proper care of Mr. Frye's PII, leading to its exposure as a direct result of Defendant's inadequate security measures. In December of 2021, Plaintiff Frye received a notification letter from Defendant stating that his PII was stolen, which included Mr. Frye's "name, address, telephone number, email address, date of birth, race, ethnicity, gender, disability status, medical notes, performance and disciplinary notes, Social Security number, health insurance plan election, income amount, and retirement contribution amounts."

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

The letter also noted the possibility of the hackers accessing or removing records that included direct deposit bank account information.

21. The letter also offered one year (12 months) of credit monitoring through Experian IdentityWorks, which was and continues to be ineffective for Mr. Frye and other Class members. The Experian credit monitoring would have shared Mr. Frye's information with third parties and could not guarantee complete privacy of his sensitive PII.

22. In the months and years following the Data Breach, Mr. Frye and the other Class members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, requests for services taken out in employees' names, fraudulent bank account charges, and targeted advertising without consent.

23. Plaintiff Frye greatly values his privacy, especially in the administration of his finances, and would not have given his PII to McMenamins if he had known that it was going to maintained in McMenamins' database without adequate protection.

E. Defendant

24. Defendant McMenamins, Inc. is a Portland, Oregon company that operates hotels, movie theaters, event spaces, bars, and restaurants throughout Oregon and Washington. McMenamins registered its headquarters at 430 North Killingsworth Street, Portland, Oregon 97217. McMenamins' corporate policies and practices, including those used for data privacy, are established in, and emanate from the state of Oregon.

JURISDICTION AND VENUE

25. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

26. The Court has personal jurisdiction over Defendant because Defendant conducts business in the state of Washington.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

27. Venue is proper in this district under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the Class's claims occurred in this District.

FACTS

28. Defendant owns a chain of brewpubs, breweries, music venues, historic hotels, and theater pubs in Oregon and Washington. Many of its locations are in rehabilitated historical properties, and the Brewer's Association has named McMenamins as one of the fifty largest craft breweries in the United States.[1] As part of its business, Defendant employs thousands of people throughout Oregon and Washington—and consequently was entrusted with, and obligated to safeguard and protect the Private Information of Plaintiffs and the Class in accordance with all applicable law.

29. In December of 2021, Defendant first learned of an incident in which a ransomware attack allowed unauthorized access to the PII contained within the McMenamins network of past and present employees from January 1, 1998 to December 12, 2021. The information lost included names, addresses, Social Security numbers, bank account numbers, and other confidential billing information. Defendant posted the following notice on its website:[2]

> NOTICE OF DATA BREACH
> SPECIAL ATTENTION: PREVIOUS EMPLOYEES 1/1/1998 – 6/30/2010
>
> Updated: December 30, 2021
>
> In early December 2021, McMenamins suffered a data breach that may have affected the personal information of certain current and previous employees. We regret this incident and want to make sure that potentially affected individuals have information and our support to protect their information.

[1] *See* Portland Business Journal, *Oregon Places 4 Breweries on List of Nation's 50 Biggest Beermakers*, THE BUS. JOURNALS (Apr. 14, 2009), https://www.bizjournals.com/portland/stories/2009/04/13/daily10.html.

[2] McMenamins, Inc., *Notice of Data Breach*, (Dec. 30, 2021), https://www.mcmenamins.com/notice-of-data-breach [hereinafter *Data Breach Notice*].

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

This notice provides information specifically for individuals employed by McMenamins within the January 1, 1998 – June 30, 2010 time period for whom the company does not have contact information, along with general information about the incident. To help protect current and past employees' identity, we are providing a 12-month membership of Experian's® IdentityWorksSM. See details below.

For individuals employed July 30, 2010 – December 12, 2021, McMenamins mailed individual notices with the same general information and individual codes so you can enroll in identity and credit monitoring and protection services. These notices were sent between December 21 and December 30 of 2021.

We also established a call center to answer questions about this incident: (888) 401-0552.

For customer and other related FAQ's, please click here.

What Happened

On December 12, 2021, McMenamins suffered a ransomware attack. As soon as we realized what was happening, we blocked access to our systems to contain the attack that day. It appears that cybercriminals gained access to company systems beginning on December 7 and through the launch of the ransomware attack on December 12. During this time, they installed malicious software on the company's computer systems that prevented us from using or accessing the information they contain.

Which Employees Were Affected and What Information Was Involved

We have determined that the hackers stole certain business records, including human resources/payroll data files for at least some individuals who were previously employed by McMenamins between January 1, 1998 and June 30, 2010. We have not been able to recover these files or contact information for these previous employees. Out of abundance of caution and for the purposes of providing this notice and credit monitoring support, we are assuming that all previous employees during this time period were potentially affected.

In addition, the hackers stole the same type of human resources files for persons employed by McMenamins between July 1, 2010 and

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

December 12, 2021. Because we were able to recover the contact information for these individuals, McMenamins mailed to them individual notices containing the same general information about the incident and individual information for enrolling in identity and credit monitoring and protection services.

The affected files potentially contained the following categories of personal information for all potentially affected current and past employees: name, address, telephone number, email address, date of birth, race, ethnicity, gender, disability status, medical notes, performance and disciplinary notes, Social Security number, health insurance plan election, income amount, and retirement contribution amounts. Although it is possible that the hackers accessed or took records with direct-deposit bank account information, we do not have any indication that they did, in fact, do so.

What McMenamins Is Doing

McMenamins is investigating the attack and working to get business back online. We notified the FBI and are cooperating with their efforts. We are working with an experienced cybersecurity investigation firm to understand the attack, restore our systems, and enhance our security. We have notified the Attorney Generals of Oregon and Washington, major credit reporting bureaus, and the news media.

As noted above, we have sent individual notice letters to the first two categories of employees listed above – employees as of December 12, 2021, and individuals employed at some point between July 1, 2010 and December 11, 2021. We are providing identity theft and credit monitoring and protection services to all current and previous employees between January 1, 1998 and December 12, 2021, as explained below and strongly encourage all persons employed during this time range to enroll in these services. If we learn additional information affecting current or past employees, we will provide updated notice.

What You Can Do to Protect Your Information

You should be vigilant when responding to communications from unknown sources and regularly monitor your financial accounts and healthcare information for any unusual activity. If you notice any unusual activity, you should immediately notify your financial institutions (e.g., your bank) and your health insurer. A set of recommendations for identity theft protection and details on how to

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

> place a fraud alert or a security freeze on your credit file is posted here. If you suspect that you are the victim of identity theft or fraud, you should notify your state Attorney General's Office and the Federal Trade Commission. These agencies' contact information is available here.
>
> To help protect current and past employees' identity, we are providing a 12-month membership of Experian's® IdentityWorksSM. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow these steps . . .

30. Upon learning of the Data Breach in December of 2021, Defendant investigated. Defendant still has not provided an estimate of how many plan participants were affected by the Data Breach.

31. On December 30, 2021 Defendant announced that it first learned of a ransomware attack that allowed on ore more unauthorized parties to access their systems. The 2021 Notice disclosed that unauthorized users stole sensitive employee information.

32. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected employees, which resulted in Plaintiffs and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

33. McMenamins' notice of the Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach occurred system-wide, whether servers storing information were accessed, and how many individuals were affected by the Data Breach. Even worse, McMenamins offered only one year of identity monitoring for Plaintiffs and Class members, which required their disclosure of additional PII with which McMenamins had just demonstrated it could not be trusted with.

34. Plaintiffs and Class members' PII is likely for sale to criminals on the dark web, meaning that unauthorized parties have accessed and viewed Plaintiffs' and Class members'

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

unencrypted, unredacted information, including names, addresses, email addresses, dates of birth, Social Security numbers, bank account information, and more.

35. The Breach occurred because Defendant failed to take reasonable measures to protect the Personal Identifiable Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this release of information, despite repeated warnings to companies about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

36. Defendant disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class members was compromised through unauthorized access. Plaintiffs and Class members have a continuing interest in ensuring that their information is and remains safe.

A. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Employees' Private Information

37. McMenamins acquires, collects, and stores a massive amount of its employees' protected PII, including financial information and other personally identifiable data.

38. As a condition of engaging in employment, McMenamins requires that these employees entrust them with highly confidential Private Information.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' Private Information, McMenamins assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class members' Private Information from disclosure.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

40. Defendant had obligations created by industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

41. Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information.

42. Plaintiffs and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

43. Prior to and during the Data Breach, Defendant promised its employees, directly and impliedly, that their Private Information would be kept confidential.

44. Defendant's failure to provide adequate security measures to safeguard employee Private Information is especially egregious because Defendant was on notice that scammers frequently target businesses with the goal of gaining access to and exploiting employee information.

45. In fact, Defendant has been on notice for years that Plaintiffs' and all other Class members' PII was a target for malicious actors. Despite such knowledge, McMenamins failed to implement and maintain reasonable and appropriate security measures to protect Plaintiffs' and Class members' PII from unauthorized access McMenamins should have anticipated and guarded against.

46. Defendant was also on notice that ransomware attacks on businesses are increasingly common. For example, the Verizon Business 2021 Data Breach Investigations Report saw and over 200 percent increase in ransomware attacks affecting businesses than in 2020.[3]

[3] Verizon, *Results and Analysis*, 2021 Data Breach Investigations Report (2021), https://www.verizon.com/business/resources/reports/dbir/

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

47. The Department of Labor ("DOL") has also warned retirement plan administrators about the importance of protecting consumer information, noting that the "DOL's No. 1 concern is whether the firm is meeting current standards and addressing vulnerabilities, particularly as they change and evolve. 'If we were in looking at a recordkeeper or a TPA for cybersecurity, we'd want to see that there's a formal well-documented cybersecurity program, that there are procedures, guidelines and standards in place, that they're regularly updated and that they're actually implemented'"[4]

48. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[5] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[6] That trend continues.

49. The average time to identify and contain a data breach is 287 days,[7] with some breaches going unrecognized for months leading to costly recover efforts and financial impact. Additionally, the median cost per US consumer incurred on each fraud-related data breach incident in 2020 was $450.[8] Data breaches and identity theft have a crippling effect on individuals and detrimental impact on the economy as a whole.[9]

50. A 2021 study conducted by Verizon showed that the most prevalent patterns in the accommodation and food services industry related to data breaches were System Intrusion, Social

---

[4] *Id.*
[5] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.
[6] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.
[7] IBM SECURITY, COST OF A DATA BREACH REPORT 6 (2021) [hereinafter COST OF A DATA BREACH REPORT]
[8] Insurance Information Institute, *Facts + Statistics: Identity Theft and Cybercrime* (2020), https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#top
[9] *Id.*

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

Engineering and Basic Web Application Attacks,.[10] The majority of these incidents involve the direct installation of malware by an attacker.[11]

51. PII related data breaches continued to rapidly into 2021 when McMenamins was breached.[12]

52. Almost half of the data breaches globally are caused by internal errors, either human mismanagement of sensitive information, or system errors.[13] Cybersecurity firm Proofpoint reports that since 2020, there has been an increase of internal threats through the misuse of security credentials or the negligent release of sensitive information.[14] To mitigate these threats, Proofpoint recommends that firms take the time to train their employees about the risks of such errors.[15]

53. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[16]

54. To prevent and detect unauthorized access, including the systems changes that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

---

[10] *Accommodation and Food Services*, VERIZON 2021 DIBR DATA BREACH SURVEY (2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/financial-services-data-breaches/.

[11] *Id.*

[12] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.

[13] COST OF A DATA BREACH REPORT, *supra* note 8, at 30.

[14] *The Human Factor 2021*, PROOFPOINT (July 27, 2021), https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf.

[15] *Id.*

[16] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

55. To prevent and detect unauthorized access to their systems, including the unauthorized access that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[17]

56. To prevent and unauthorized access, including the access by other plan administrators that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**

- Apply the latest security updates

[17] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

- Use threat and vulnerability management
- Perform regular audit; remove privilege credentials;
- **Thoroughly investigate and remediate alerts**
- Prioritize and treat commodity malware infections as potential full compromise
- **Include IT Pros in security discussions**
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
- use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events
- **Harden infrastructure**
- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[18]

57. These are basic, practical email security measures that every business, not only those who handle sensitive financial information, should be doing. McMenamins should be doing

[18] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

even more. But by adequately taking these common-sense solutions, McMenamins could have prevented this Data Breach from occurring.

58. Charged with handling sensitive PII including financial information, McMenamins knew, or should have known, the importance of safeguarding its employees' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on McMenamins' employees as a result of a breach. McMenamins failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

59. With respect to training, McMenamins specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

60. The PII was also maintained on McMenamins computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's negligently maintained systems. The mechanism of the unauthorized access—including the improper security of network hardware within McMenamins facilities—and the potential for improper disclosure of Plaintiffs' and Class members' PII was a known risk to McMenamins, and thus McMenamins was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

B. The Monetary Value of Privacy Protections and Private Information

61. The fact that Plaintiffs' and Class members' Private Information was stolen—and is likely presently offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

62. At all relevant times, Defendant was well aware that Private Information it collects from Plaintiffs and Class members is highly sensitive and of significant property value to those who would use it for wrongful purposes.

63. Private Information is a valuable property right that is an important commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft and financial fraud.[19] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive financial information on multiple underground Internet websites, commonly referred to as the dark web.

64. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[20]

[19] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

20 *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

65. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[21]

66. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[22]

67. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[23] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

68. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[24]

---

[21] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

[22] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

23 *Web's Hot New Commodity*, *supra* note 17.

24 *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

69. The value of Plaintiffs' and Class members' Private Information on the black market is substantial. Sensitive financial information can sell for more than $1000.[25] This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's information.

70. The ramifications of McMenamins' failure to keep its employees' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

71. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[26] This gives thieves ample time to make fraudulent charges under the victim's name.

72. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting businesses in the United States.

73. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the ransomware attack into their systems and, ultimately, the theft of their employees' Private Information.

74. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that

[25] *See* Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACY AFFAIRS (Nov. 21, 2021), https://www.privacyaffairs.com/dark-web-price-index-2021/

[26] *See Medical ID Theft Checklist*, IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[27] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[28] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiffs and Class members that was misused.

75. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

76. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment information was not involved in the Data Breach of some individuals' information, the unauthorized parties could use Plaintiffs' and Class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in fraudulent activity.

77. Acknowledging the damage to Plaintiffs and Class members, Defendant instructed employees like Plaintiffs to "be vigilant when responding to communications from unknown sources and regularly monitor your financial accounts and healthcare information for any unusual activity. If you notice any unusual activity, you should immediately notify your financial institutions (e.g., your bank) and your health insurer." Plaintiffs and the other Class members now face a greater risk of identity theft.

---

[27] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[28] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

78. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names. Plaintiffs and Class members have a property interest in their information and were deprived of this property when it was released to unauthorized actors through the negligent maintenance of Defendant's systems.

C. McMenamins Failed to Comply with FTC Guidelines

79. McMenamins was prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

80. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[29]

81. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[30] The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

82. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require

[29] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

[30] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[31]

83. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. McMenamins was at all times fully aware of its obligation to protect the Private Information of employees. McMenamins was also aware of the significant repercussions that would result from its failure to do so.

D. Damages to Plaintiffs and the Class

85. Plaintiffs and the Class have been damaged by the compromise of their Private Information in the Data Breach.

86. The ramifications of McMenamins' failure to keep employees' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Victims of data breaches are more likely to become victims of identity fraud.[32]

87. In addition to its obligations under state laws and regulations, Defendant owed a common law duty to Plaintiffs and Class members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and

[31] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter Start with Security].

[32] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

88. Defendant further owed and breached its duty to Plaintiffs and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

89. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiffs' and Class members' Private Information as detailed above, and Plaintiffs are now at a heightened and increased risk of identity theft and fraud.

90. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some individuals victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

91. Some of the risks associated with the loss of personal information have already manifested themselves in respect to Plaintiffs. Plaintiffs Leonard, Frazier, and Frye received a cryptically written notice letter from Defendant stating that their information was released, and that they should remain vigilant of fraudulent activity on their accounts, with no other explanation of where this information could have gone, or who might have access to it. Because Defendant directed Plaintiffs to monitor their accounts and otherwise mitigate their damages, Plaintiffs have been forced to spend hours on the phone trying to determine what negative effects may occur from the loss of their personal information.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

92. Plaintiffs and the Class have suffered or face a substantial risk of suffering out-of-pocket losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, and similar identity theft.

93. Plaintiffs Frazier and deGrasse, as well as other Class members have experienced a slew of phishing emails and text messages, attempts by cybercriminals to lure Class members into divulging more sensitive information that can be used to perpetrate further identity theft attacks.

94. Additionally, Plaintiff deGrasse experienced fraudulent charges on his Visa credit card account, resulting in time spent mitigating these identity theft attempts through speaking with customer service representatives, reversing any fraudulent charges, and activating a new Visa credit card. This is just one example of the types of identity theft and fraud that Plaintiffs and Class members will experience in the coming months as a result of the data breach.

95. Plaintiffs and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

96. Plaintiffs and Class members did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in their agreements with McMenamins.

97. Plaintiffs and Class members would not have released their information to Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from theft.

98. Plaintiffs and the Class will continue to spend significant amounts of time to monitor their financial accounts for misuse.

99. The theft of Social Security Numbers, which were purloined as part of the Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration ("SSA")

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

warns that "[i]dentity theft is one of the fastest growing crimes in America."[33] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[34] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[35]

100. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[36]

101. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. Private Information can be used to submit false insurance claims. As a result, Plaintiffs and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit for an indefinite duration. For Plaintiffs and Class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

33 *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

34 *Id.*

35 *Id.*

36 *Id.*

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

102. As a result of the Data Breach, Plaintiffs' and Class members' Private Information has diminished in value.

103. The Private Information belonging to Plaintiffs and Class members is private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed information about Plaintiffs and the class that was of an extremely personal, sensitive nature as a direct result of its inadequate security measures.

104. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiffs' and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

105. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect employee data.

106. Defendant did not properly train their employees to identify and avoid unauthorized access to the network.

107. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs' and Class members' Private Information.

108. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

109. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[37]

110. Other than offering 12 months of credit monitoring, Defendant did not take any measures to assist Plaintiffs and Class members other than telling them to simply do the following:

- remain vigilant for incidents of fraud and identity theft;
- review account statements and monitor credit reports for unauthorized activity;
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiffs' and Class members' Private Information.

111. Defendant's failure to adequately protect Plaintiffs' and Class members' Private Information has resulted in Plaintiffs and Class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as McMenamins' Data Breach Notice indicates, it is putting the burden on Plaintiffs and Class members to discover possible fraudulent activity and identity theft.

[37] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

112. While Defendant offered one year of credit monitoring, Plaintiffs could not trust a company that had already breached their data. The credit monitoring offered from Experian does not guarantee privacy or data security for Plaintiffs, who would have to expose their information once more to get monitoring services. Thus, to mitigate harm, Plaintiffs and Class members are now burdened with indefinite monitoring and vigilance of their accounts.

113. Moreover, the offer of 12 months of identity monitoring to Plaintiffs and Class members is woefully inadequate. While some harm has already begun, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[38] This is especially true for many kinds of financial identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

114. Plaintiffs and Class members have been damaged in several other ways as well. Plaintiffs and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiffs and Class members must now and indefinitely monitor their financial and other accounts closely to guard against fraud. This is a burdensome and time-consuming activity. Plaintiffs and Class members have spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiffs and Class members also suffered a loss of the inherent value of their Private Information.

115. The Private Information stolen in the Data Breach can be misused on its own, or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit

[38] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

116. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;
- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members; and
- Anxiety and distress resulting fear of misuse of their Private Information.

117. In addition to a remedy for the economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

CLASS ACTION ALLEGATIONS

118. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

119. Plaintiffs bring this action as a class action pursuant to Federal Rule of Civil Procedure 23 and seek certification of the following Nationwide Class and state subclasses (collectively referred to herein as the "Class"), subject to amendment based on information obtained through discovery:

Nationwide Class

> All persons nationwide whose Private Information was compromised as a result of the Data Breach discovered on or about December of 2021 who had their information inputted to McMenamins systems and were sent notice of the Data Breach (individuals employed from July 30, 2010 to December 12, 2021). Additionally, all persons nationwide whose Private Information was compromised as a result of the Data Breach discovered on or about December of 2021 who had their information inputted to McMenamins systems and were affected, but did not receive a notice letter (individuals employed from January 1, 1998 to June 30, 2010).

Washington Subclass

> All persons residing in the state of Washington whose Private Information was compromised as a result of the Data Breach discovered on or about December of 2021 who had their information inputted to McMenamins systems and were sent notice of the Data Breach (individuals employed from July 30, 2010 to December 12, 2021). Additionally, all persons residing in the state of Washington whose Private Information was compromised as a result of the Data Breach discovered on or about December of 2021 who had their information inputted to McMenamins systems and were affected, but did not receive a notice letter (individuals employed from January 1, 1998 to June 30, 2010).

Oregon Subclass

> All persons residing in the state of Oregon whose Private Information was compromised as a result of the Data Breach discovered on or about December of 2021 who had their information

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

> inputted to McMenamins systems and were sent notice of the Data Breach (individuals employed from July 30, 2010 to December 12, 2021). Additionally, all persons residing in the state of Oregon whose Private Information was compromised as a result of the Data Breach discovered on or about December of 2021 who had their information inputted to McMenamins systems and were affected, but did not receive a notice letter (individuals employed from January 1, 1998 to June 30, 2010).

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

120. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

121. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class numbers in the thousands.

122. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant properly implemented its purported security measures to protect Plaintiffs' and the Class's Private Information from unauthorized capture, dissemination, and misuse;

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiffs' and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class's Private Information;
- Whether Defendant was negligent in failing to properly secure and protect Plaintiffs' and the Class's Private Information;
- Whether Defendant was unjustly enriched by its actions; and
- Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

123. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

124. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiffs.

125. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class they seek to represent, they have retained counsel competent and experienced

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

126. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

127. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

128. Class certification is also appropriate because this Court can designate particular claims or issues and designate multiple subclasses, if necessary, for class-wide treatment pursuant to Fed. R. Civ. P. 23(c)(4).

129. No unusual difficulties are likely to be encountered in the management of this action as a class action.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

130. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

131. Upon Defendant's accepting and storing the Private Information of Plaintiffs and the Class in their computer systems and on their networks, Defendant undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

132. Defendant owed a duty of care not to subject Plaintiffs' and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiffs and the Class were foreseeable and probable victims of any inadequate security practices.

133. Defendant owed numerous duties to Plaintiffs and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

134. Defendant also breached its duty to Plaintiffs and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

malicious third party to gather Plaintiffs' and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

135. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches.

136. Defendant knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class members' Private Information.

137. Defendant breached their duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and Class members' Private Information.

138. Because Defendant knew that a breach of their systems would damage thousands of their employees, including Plaintiffs and Class members, Defendant had a duty to adequately protect their data systems and the Private Information contained thereon.

139. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

140. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

141. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential Private Information.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

142. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiffs' and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

143. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;
- Failing to adequately monitor the security of Defendant's networks and systems;
- Allowing unauthorized access to Class members' Private Information;
- Failing to detect in a timely manner that Class members' Private Information had been compromised; and
- Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

144. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiffs' and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' Private Information during the time it was within Defendant's possession or control.

145. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

and failing to provide Plaintiffs and Class members with timely notice that their sensitive Private Information had been compromised.

146. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

147. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

148. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
Breach of Contract
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

149. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

150. Plaintiffs and other Class members entered into valid and enforceable express contracts with Defendant under which Plaintiffs and other Class members agreed to provide their Private Information to Defendant, and Defendant impliedly, if not explicitly, agreed to protect Plaintiffs and Class members' Private Information.

151. To the extent Defendant's obligation to protect Plaintiffs' and other Class members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and other Class members' Private Information, including in accordance with trade regulations; federal, state and local laws; and industry standards. Plaintiffs and Class members would not have entered into these contracts with Defendant without the

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

understanding that their Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

152. A meeting of the minds occurred, as Plaintiffs and Class members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

153. The protection of Plaintiffs' and Class members' Private Information were material aspects of Plaintiffs' and Class members' contracts with Defendant.

154. Defendant's promises and representations described above relating to industry practices, and about Defendant' purported concern about their employees' privacy rights became terms of the contracts between Defendant and their employees, including Plaintiffs and other Class members. Defendant breached these promises by failing to comply with reasonable industry practices.

155. Plaintiffs and Class members read, reviewed, and/or relied on statements made by or provided by McMenamins and/or otherwise understood that McMenamins would protect its patients' Private Information if that information were provided to McMenamins

156. Plaintiffs and Class members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

157. As a result of Defendant's breach of these terms, Plaintiffs and other Class members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

Plaintiffs and other Class members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

158. Plaintiffs and Class members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
Breach of Implied Contract
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

159. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

160. This count is brought by Plaintiffs alternatively to Count II.

161. Through their course of conduct, Defendant, Plaintiffs, and Class members entered into implied contracts for employment, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' Private Information.

162. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendant when he first entered into the employment agreement with Defendant.

163. The valid and enforceable implied contracts to provide labor services that Plaintiffs and Class members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant creates on its own from disclosure.

164. When Plaintiffs and Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

165. Defendant required Class members to provide their Private Information as part of Defendant's regular employment practices. Plaintiffs and Class members accepted Defendant's offers and provided their Private Information to Defendant.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

166. In entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

167. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide labor services to Plaintiffs and Class members; and (b) protect Plaintiffs' and the Class members' Private Information provided to obtain such benefits of such services.

168. Both the provision of labor services and the protection of Plaintiffs' and Class members' Private Information were material aspects of these implied contracts.

169. The implied contracts for the provision of labor services—contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter.

170. Employees value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining such services. Plaintiffs and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

171. A meeting of the minds occurred, as Plaintiffs and Class members agreed and provided their Private Information to Defendant and/or its affiliated companies with an understanding that their private information would be protected.

172. Plaintiffs and Class members performed their obligations under the contract when they agreed to employment and provided their Private Information.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

173. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

174. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiffs' and Class members Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiffs' and Class members private information as set forth above.

175. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

176. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, Class members, nor any reasonable person would have agreed to entrust Defendant with their employment information.

177. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

178. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

179. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

COUNT IV
Unjust Enrichment/Quasi-Contract
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

180. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

181. Defendant knew that Plaintiffs and Class members conferred a benefit on them and accepted or retained that benefit. Defendant profited from Plaintiffs' purchases and used Plaintiffs' and Class member's Private Information for business purposes.

182. Defendant failed to secure Plaintiffs and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiffs and Class members' Private Information provided.

183. Defendant acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

184. If Plaintiffs and Class members knew that Defendant would not secure their Private Information using adequate security, they would not have agreed to release this information to Defendant.

185. Plaintiffs and Class members have no adequate remedy at law.

186. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on them.

187. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

COUNT V
Breach of Fiduciary Duty
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

188. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

189. In providing their Private Information to Defendant, Plaintiffs and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiffs and Class members to safeguard and keep confidential that Private Information.

190. Defendant accepted the special confidence Plaintiffs and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiffs' personal information as included in the Data Breach notification letter.

191. In light of the special relationship between Defendant and Plaintiffs and Class members, whereby Defendant became a guardian of Plaintiffs' and Class members Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its employees, including Plaintiffs and Class members for the safeguarding of Plaintiffs and Class member's Private Information.

192. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of its employment relationship, in particular, to keep secure the Private Information of its employees.

193. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to protect the integrity of the systems containing Plaintiffs' and Class member's Private Information.

194. Defendant breached its fiduciary duties to Plaintiffs and Class members by otherwise failing to safeguard Plaintiffs' and Class members' Private Information.

195. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i)

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cyber-Attack and Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

196. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Breach of Confidence
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

197. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

198. At all times during Plaintiffs and Class members' interactions with Defendant, Defendant was fully aware of the confidential, novel, and sensitive nature of Plaintiffs' and the Class members' Private Information that Plaintiffs and Class members provided to Defendant.

199. As alleged herein and above, Defendant's relationship with Plaintiffs and Class members was governed by expectations that Plaintiffs and Class members' Private Information

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

200. Plaintiffs and Class members provided their respective Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

201. Plaintiffs and Class members also provided their respective Private Information to Defendant with the explicit understanding that Defendant would take precautions to protect that Private Information from unauthorized disclosure, such as following basic principles of information security practices.

202. Defendant voluntarily received in confidence Plaintiffs and Class members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

203. Due to Defendant's failure to prevent, detect, and/or avoid the Security Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiffs' and Class members' Private Information, Plaintiffs' and Class members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class members' confidence, and without their express permission.

204. But for Defendant's disclosure of Plaintiffs' and Class members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Security Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' Private Information, as well as the resulting damages.

205. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class members' Private Information. Defendant knew or should have known their security systems were

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

insufficient to protect the Private Information that is coveted by thieves worldwide. Defendant also failed to observe industry standard information security practices.

206. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT VI
Bailment
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

207. Plaintiffs incorporate by reference all of the above paragraphs, as though fully set forth herein.

208. Plaintiffs and Class members delivered and entrusted their Personal Information to Defendant for the sole purpose of initiating employment with Defendant.

209. In delivering their Personal Information to Defendant, Plaintiffs and Class members intended and understood that Defendant would adequately safeguard their personal and financial information.

210. Defendant accepted possession of Plaintiffs and Class members' Personal Information. By accepting possession, Defendant understood that Plaintiffs and Class members expected Defendant to safeguard their personal and financial information adequately. Accordingly, a bailment was established for the mutual benefit of the parties.

211. During the bailment, Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care, diligence, and prudence in protecting their Personal Information.

212. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class members' Personal Information, resulting in the unlawful and unauthorized access to and misuse of such information.

213. Defendants further breached their duty to safeguard Plaintiffs' and Class members' Personal Information by failing to notify them individually in a timely and accurate manner that their information had been breached and compromised.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

214. As a direct and proximate result of Defendant's breach of duty, Plaintiffs and Class members suffered consequential damages that were reasonably foreseeable to Defendants, including but not limited to the damages set forth herein.

COUNT VII
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT, Wash. Rev. Code An. §§ 19.86.020, *et seq.*,
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Washington Subclass)

215. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

216. McMenamins is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

217. McMenamins advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

218. McMenamins engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. By Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Washington Subclass members' Personal Information, which was a direct and proximate cause of the data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the data breach

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class members' PII, including by implementing and maintaining reasonable security measures

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act.

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PII; and

g. Omitting suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act.

219. McMenamins' representations and omissions were material because they were likely to deceived reasonable employees about the adequacy of McMenamins' data security and ability to protect the confidentiality of employees' PII.

220. McMenamins acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Class members' rights. Numerous past data breaches put it on notice that its security and privacy protections were inadequate.

221. McMenamins' conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the thousands of Washingtonians affected by the data breach.

222. As a direct and proximate result of McMenamins' unfair or deceptive acts or practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft ; and loss of value of their PII.

223. Plaintiffs and Class members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

COUNT VIII
DECLARATORY RELIEF
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

224. Plaintiffs repeat and reallege each of the above paragraphs as though fully set forth herein.

225. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

226. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their PII will occur in the future.

227. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect McMenamins employees' PII.

228. Defendant still possesses the PII of Plaintiffs and the Class.

229. Defendant has made no announcement that it has changed its data storage or security practices relating to the PII.

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

230. Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

231. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at McMenamins. The risk of another such breach is real, immediate, and substantial.

232. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at McMenamins, Plaintiffs and Class members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

233. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at McMenamins, thus eliminating the additional injuries that would result to Plaintiffs and Class members, along with other employees whose PII would be further compromised.

234. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that McMenamins implement and maintain reasonable security measures, including but not limited to the following:

- Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on McMenamins systems on a periodic basis, and ordering McMenamins to promptly correct any problems or issues detected by such third-party security auditors;
- engaging third-party security auditors and internal personnel to run automated security monitoring;

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

- auditing, testing, and training its security personnel regarding any new or modified procedures;
- purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;
- conducting regular database scans and security checks; and
- routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims so triable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

a. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to employee data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660

e. Ordering Defendant to pay for not less than three (3) years of credit monitoring services for Plaintiffs and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and such other and further relief as this court may deem just and proper.

DATED May 13, 2022.

Respectfully submitted,

BRESKIN JOHNSON & TOWNSEND, PLLC

By: *s/ Cynthia Heidelberg*
Cynthia J Heidelberg, WSBA #44121
1000 Second Avenue, Suite 3670
Seattle, WA 98104
(206) 652-8660 Fax (206) 652-8290
cheidelberg@bjtlegal.com

Nicholas A. Migliaccio (*admitted pro hac vice*)
Jason S. Rathod (*admitted pro hac vice*)
MIGLIACCIO & RATHOD LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
221 W. Monroe Street, Suite 2100
T: 919-600-5000
gklinger@milberg.com

CERTIFICATE OF SERVICE

I hereby certify that on May 13, 2022, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all parties registered on the CM/ECF system. All other parties (if any) shall be served in accordance with the Federal Rules of Civil Procedure.

s/ Julia Wolfe
Julia Wolfe, Legal Assistant

BRESKIN | JOHNSON | TOWNSEND PLLC
1000 Second Avenue, Suite 3670
Seattle, Washington 98104 Tel: 206-652-8660